W3C 勧告準拠の XML 署名基盤 技術開発とリファレンス提供

森 拓也 <tk-mori@isd.nec.co.jp>, 宮内 幸司 <k-miyauc@isd.nec.co.jp>,
杉山 高弘 <sugiyama@isd.nec.co.jp>

日本電気株式会社
インターネットソフトウェア開発本部

政府は、2003年度までに行政の効率化や国民負担の軽減を目標に行政手続きを電子化する電子政府の基盤を構築することを目指しており、電子申請文書や電子化公文書等の改竄防止を実現する電子署名技術、および、情報の漏洩防止のための電子文書暗号化技術の重要性が高まってきている。また、電子文書を交換するフォーマットとして、XML(eXtensible Markup Language)がデファクト標準としてますます普及してきており、IETF/W3Cは共同で、電子署名フォーマットとしてXMLを基盤としたXML署名仕様の策定を進めており、電子署名文書のデファクト標準となることが予想されている。本技術開発は、XML署名仕様に基づいた標準電子署名基盤を開発することにより、電子政府システムや民間の電子商取引の普及を促進することを目的とする。

１．はじめに

ミレニアム・プロジェクトとしてその基盤が構築される電子政府は、行政の効率化や国民負担の軽減を目標に、申請届出手続きや政府調達など行政手続きの電子化を実現しようとしている。そのため、電子申請や電子調達で取り交わされる電子文書や省庁間で交換される電子化公文書の改竄防止を保証する電子署名技術、および情報の漏洩防止を保証する電子文書暗号技術が重要になってきている。

電子政府や電子商取引などの多くのシステムで、電子文書を交換するための標準フォーマットとして XML が使用されており、今後も、XML 電子文書の交換においてデファクト標準としてますます普及することが予想される。

本技術開発は、電子政府システムや民間の商取引システム等における情報セキュリティ確保の一環として、電子文書の改竄の防止や情報漏洩の防止を保証する電子署名技術､電子文書暗号化技術を開発し､その妥当性を検証するものである。その結果を踏まえ、これらの技術のデファクト標準化を図るとともに、民間の範となる方式を示すことで、広く民間を含むシステム間での電子署名文書、電子暗号文書の相互運用性を確保し、電子政府システム、電子商取引の普及を促進することを目的とする。

２．技術開発の目標と内容

２．１　技術開発の目標

W3C/IETF は共同で、電子文書の標準と位置付けられている XML をベースとした、電子署名フォーマットの標準化仕様(XML 署名仕様：XML-Signature Syntax and Processing)の策定を進めている。本仕様は、2000 年 10 月に勧告候補となっており、仕様策定が順調に進めば 2001 年夏頃には W3C 勧告および IETF 標準となる予定である。

本技術開発は、XML Signature and Processing 勧告候補(2000 年 10 月)に基づいた、電子文書の改竄防止を保証する XML 署名機能、および電子文書の情報漏洩防止を保証する XML 暗号機能を開発することを目標とした。

２．２ 技術開発の内容

本技術開発では、W3C XML-Signature and Processing 勧告案に準拠した、汎用性のあるコンポーネント化を目指して XML 署名基盤ソフトを開発する。

本ソフトは、以下の二つの大機能から構成される。

（１）XML 署名機能

本機能は、W3Cで標準化が進められているXML-Signature Syntax and Processingに基づき、署名対象となるXML文書の一部、あるいは全部、もしくは、非XMLの文書に対して、電子署名の付与を行いXML署名文書を生成する機能と、XML署名文書に含まれる電子署名の検証を行う機能を提供する。機能開発の過程において、外部から利用するユーザの利便性を重視し、効率の良いインタフェースを構築する。具体的には以下の機能から構成される。

（ａ）XML署名文書内部データ管理機能

アプリケーションはこの機能を通じて署名対象の文書を指定し、署名計算に必要なパラメータに従って電子署名付き文書を作成する。同

じく、電子署名が付与されたXML署名文書を検証する。このとき、XML署名に係わる情報を内部データ構造として管理する。内部データ構造を操作する基本的なインタフェースも提供する。アプリケーション側からXML署名機能を使用する際に、使いやすい簡易なインタフェースとして、XML署名ユーザ利用インタフェースを設ける。

（b）XML変換機能

署名対象物に対して署名計算を行う際に、ユーザが前処理として指定することにより本機能が実行される。XML変換機能は、①表現形式は異なるが意味的に同一のものとして扱えるように正規化するXML正規化機能、②署名対象自体に署名が含まれるため署名値を計算時に無視するXMLフィルタリング機能、③署名対象文書から署名を施したい部分を取り出すXMLトランスフォーム機能、から構成される。

（c）XML署名セキュリティ管理機能

ユーザがXML署名の計算を行う際に、セキュリティ機能（ハッシュアルゴリズム、暗号アルゴリズム、公開鍵証明書取得機能、CRL取得機能等）に各種の設定を行うためのインタフェースを提供する。

（2）XML暗号機能

本機能は、暗号対象文書に対してあらかじめ指定された暗号形式、および暗号鍵を用いて暗号化を行ない、それらの暗号形式、および暗号鍵に関する情報とともに、暗号化されたコンテンツをXML暗号文書として生成する機能を提供する。また、XML暗号文書から暗号化形式と暗号鍵に関する情報、および、暗号化されたコンテンツを抽出し、元の暗号対象文書へ復号する機能を提供する。具体的には以下の機能から構成される。

（a）XML暗号文書データ管理機能

本機能は、暗号対象のXML文書と暗号形式を示す情報と暗号に用いる暗号鍵を特定する情報により暗号化・復号処理を行う機能を提供する。暗号化・複合する際の各種条件を設定するインタフェースを合わせて提供する。

（b）XML暗号セキュリティ管理機能

本機能は、暗号鍵の種類を特定する情報（例えば、公開鍵方式であるか、対称鍵方式であるか等）、鍵情報の格納形式（鍵を一意に特定する名前、鍵データの埋め込み）を特定する情報等をもとに暗号鍵情報を生成する。また、XML暗号文書に保持されている暗号鍵情報を元に、復号処理に用いる暗号鍵を取得する機能を提供する。

各機能の関係を図１に示す。

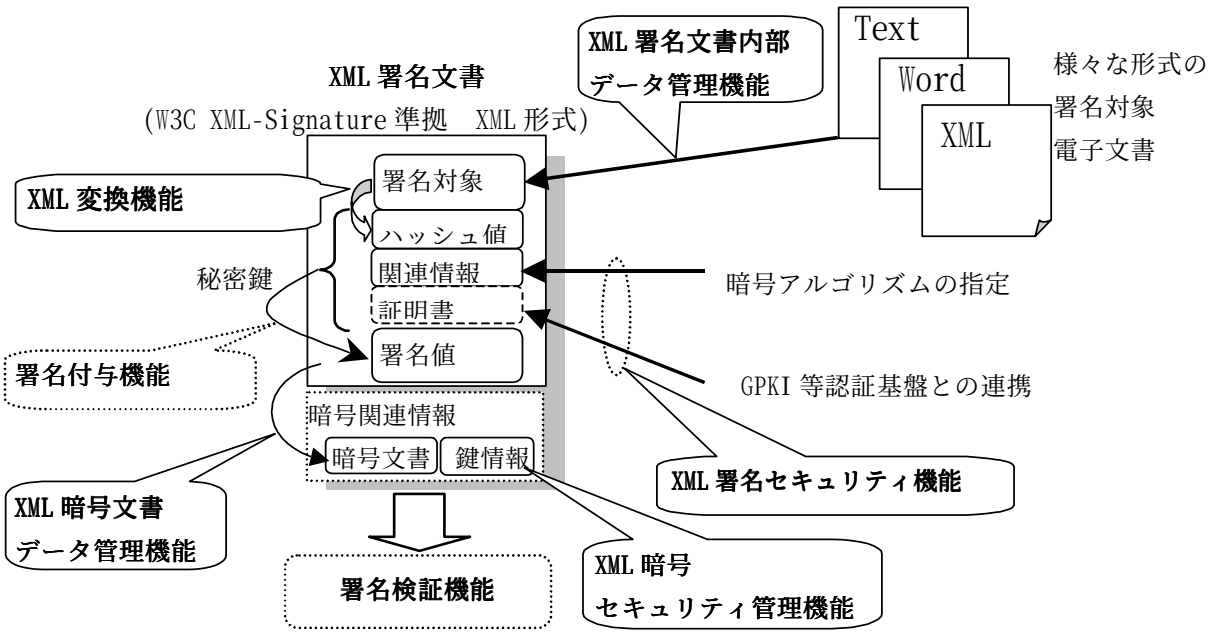

図１．XML 署名基盤技術の機能関連図

２．２．１　XML 署名機能

（１）　XML 署名機能の特長

（ａ）柔軟な署名形式

署名対象文書がXML文書の場合、署名対象文書の全体、もしくは任意の一部に対してXML署名文書を生成することができる。手形の裏書のように、Aが署名した後、Bが署名する多重署名のような複雑な署名形態に、容易に対応可能である。また、非XML文書(MS Wordファイル等)に対してXML署名文書を生成することもできるため、様々なシステム要件を満たす電子署名基盤を提供している。

（ｂ）XML変換機能

署名対象文書やXML署名文書に対する、様々な変換機能を提供する。

① XML正規化機能

XMLパーサを用いてXML文書を処理する場合、空白の個数や属性の出現順序など、XML文書の意味的な内容には影響を及ぼさないレベルで、表現上の差異が発生することがある。この表現上の差異は署名計算結果に直接影響を及ぼす。従って、XML文書を対象とした署名生成、検証処理では、この表現上の差異による影響を排除する必要がある。

W3C Canonical XML 仕様は、XML文書表現の柔軟性を損なわないことを目的に、表現形式は異なるが意味的に同一なXML文書を等価に扱うことを目的とした、XML文書正規化処理の標準仕様である。XML変換機能では、このW3C Canonical XML 仕様に準拠した正規化機能を提供しており、署名計算処理の前に正規化処理を実行することによって、XMLパーサの影響を排除することができる。

② XMLフィルタリング機能

XML文書中の任意の個所を抽出する機能である。この機能を用いて、署名対象文書の特定部分を抽出するフィルタリングスクリプトを設定することにより、署名生成後でも、署名検証に影響を与えることなく、署名対象文書の特定部分以外の変更が可能となる。

特に、後述するEnveloped Signature形式のXML署名文書の検証では、XML署名文書自体が署名計算に影響を与えないように、署名計算対象からXML署名文書自体を取り除く変換(Enveloped Signature変換)を提供している。

③ XML変換アルゴリズムユーザ登録機能

既存業務システムの制約から、署名対象文書やXML署名文書を特定なエンコーディングアルゴリズムを用いた変換を要求されることがある。このようなシステム固有のXML変換機能をXML署名生成、検証時に利用できるように、XML変換アルゴリズムユーザ登録機能を提供している。

（ｃ）セキュリティ機能登録・拡張機能

アプリケーション開発者にとって、機密性の高い業務のために、新しく開発された強固な署名アルゴリズムを利用したセキュリティ機能を採用したいという要望は増えてくる。これを実現するために、XML署名機能は、署名アルゴリズム指定のためのユーザ拡張機能、および、署名アルゴリズムの独自な鍵情報をXML署名文書に登録可能なユーザ拡張機能を有している。アプリケーション開発者による電子署名機能の独自拡張が可能な実装により、XML署名基盤ソフトはマルチプラットフォーム上での移植性に優れる。

セキュリティ機能登録・拡張機能は、JCA(Java Cryptography Architecture)、JCE(Java Cryptography Extension)等のフレームワーク技術を利用し、セキュリティ機能に依存しない利用インタフェースを提供する。

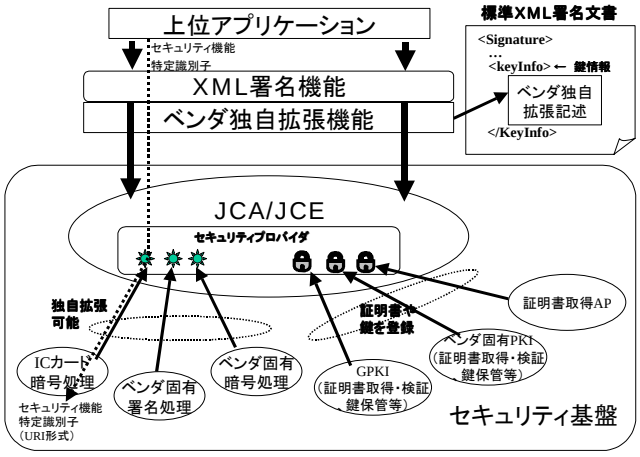

図２．セキュリティ機能登録・拡張機能

（２）　XML 署名仕様

W3C/IETF で仕様策定が進められている XML 署名仕様は、電子文書の改竄、発信者の否認、成り済まし等の防止を目的として、XML を用いた電子署名文書フォーマットを規定する XML 署名文書のシンタックスと、XML 署名文書の処理プロセス規定からなる。XML 署名仕様では、任意のフォーマットの電子文書を署名対象文書として XML 署名文書を作成でき、特に署名対象文書が XML 文書の場合、柔軟な署名文書フォーマットが利用可能である。

（ａ）XML 署名文書の三つの形式

XML署名文書は、Signatureという名前の要素をルート要素とするXMLフォーマットで表現され、Signature要素の子要素に署名値や署名時の様々な条件が保持される。

XML 署名仕様で規定される XML 署名文書の形式には、署名対象文書と XML 署名文書との関係に基づいて以下の三つの形式がある。システムの要件に基づいて、最適な形式を選択することが可能である。

① Enveloped Signature 形式

署名対象文書がXML文書の場合、XML署名文書が署名対象文書の子要素として含まれる形式である（図３）。現実の契約書やEDIシステムにおける電文等の署名の形式に適している。

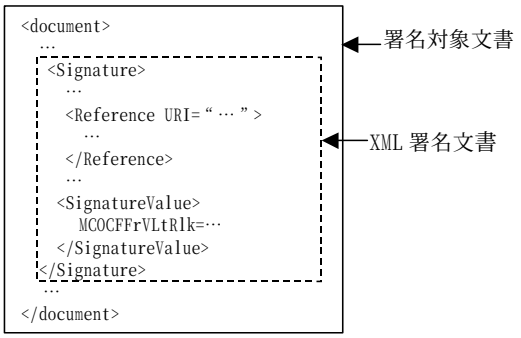

図３．Enveloped Signature 形式の XML 署名文書例

② Enveloping Signature 形式

XML署名文書の子要素として、署名対象文書が含まれる形式である（図４）。署名対象文書と署名要素を一体として管理可能なので取り扱いが容易である。

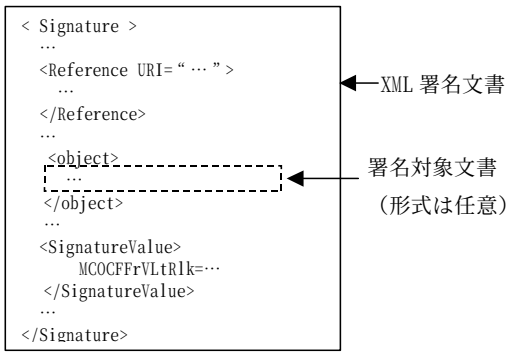

図４．Enveloping Signature 形式の XML 署名文書例

③ Detached Signature 形式

XML署名文書と、署名対象文書が包含関係をもたない形式である（図５）。署名対象文書に任意の電子ファイル（Word, Excel等）を指定可能であり、XML署名文書と独立に管理できる。

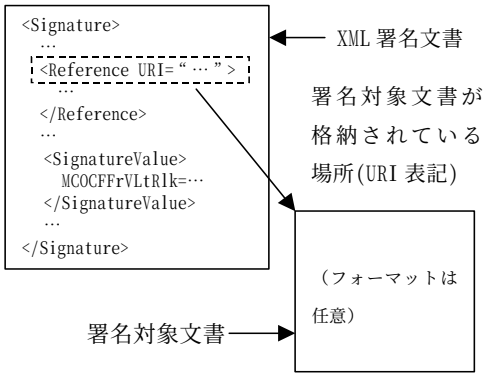

図５．Detached Signature 形式の XML 署名文書の例

（b）XML 署名文書のシンタックス

XML 署名文書は、DTD および XML スキーマを用いて定義された XML 要素で構成される。各 XML 要素は、図６で示すような階層構造をもつ。

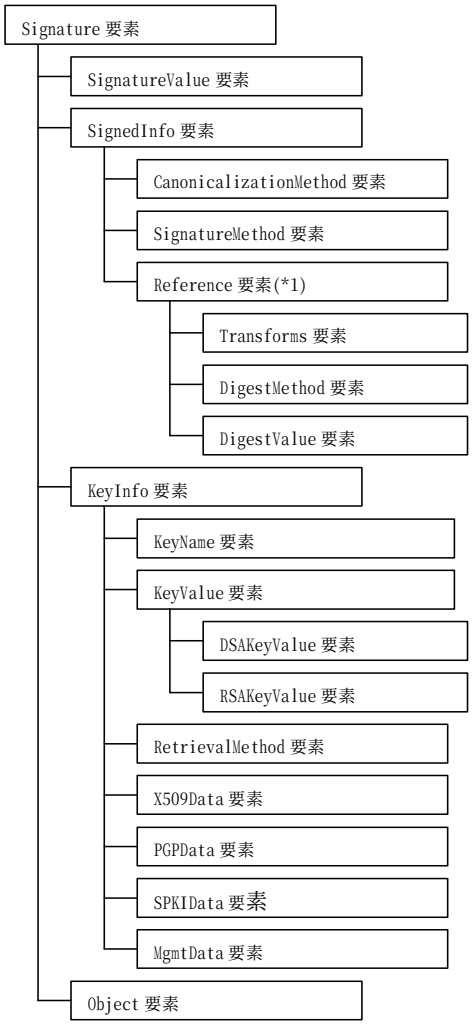

図６．XML 署名文書を構成する XML 要素

主な構成要素の役割は以下の通りである。

① Signature 要素
XML署名文書のルート要素。
② SignatureValue 要素
Base64エンコードされた署名値を保持する。
③ SignedInfo 要素
XML署名文書の生成/検証時に必要な情報（正規化アルゴリズム名、署名アルゴリズム名、および、一つ以上のダイジェスト計算関連情報等）を保持する。
④ CanonicalizationMethod 要素
署名計算を実行する前に署名対象XML文書に適用される正規化アルゴリズムの識別子を保持する。
⑤ SignatureMethod 要素
XML署名文書の生成/検証で用いる、署名アルゴリズムの識別子を保持する。
⑥ Reference 要素
ダイジェストアルゴリズムの識別子、ダイジェスト値、署名対象文書の識別子と型、ダイジェストを実行する前に実行される変換のリストを保持する。
⑦ Transforms 要素
実行する変換処理のアルゴリズムの識別子と、アルゴリズムに渡されるパラメータを保持する Transform 要素の順序付けられたリストを保持する。
⑧ DigestMethod 要素
署名対象文書に対して実行されるダイジェストアルゴリズムの識別子を保持する。
⑨ DigestValue 要素
署名対象文書に対して実行されたダイジェスト計算の結果であるダイジェスト値をBase64エンコードした値を保持する。
⑩ KeyInfo 要素
XML署名文書の検証で用いる公開鍵に関する情報を保持する。
⑪ KeyName 要素
署名検証時に用いる鍵の識別子を保持する。
⑫ KeyValue 要素
署名検証時に用いる単一の公開鍵を保持する。
⑬ RetrievalMethod 要素
外部に保持されているKeyInfoへの参照を保持する。
⑭ X509Data 要素
X509 証明書、もしくは棄却リストの情報(X.509 サブジェクト鍵識別子、X.509 サブジェクト区別名、Base64 エンコードされた X.500v3 証明書、Base64 エンコードされた X.500v2 証明書棄却リスト(CRL)、X.509Issuer 名、およびシリアルナンバ)を保持する。
⑮ PGPData 要素
PGP公開鍵ペア、およびPGP公開鍵ペアに基づいた署名に関する情報を保持する。
⑯ SPKIData 要素
SPKI公開鍵ペア、証明書、およびSPKIデータに関するその他の情報を保持する。
⑰ MgmtData 要素
DH鍵やRSA鍵暗号化等のバンド間鍵配布、もしくは協定データの識別子を保持する。
⑱ Object 要素
アプリケーションシステムによるダイジェスト計算関連情報、署名生成時の付加的情報を保持する。

（c）XML 署名文書の処理プロセス

XML 署名文書の生成処理と検証処理のプロセスを図７に示す。処理内容は以下の通りである。

[XML 署名文書の生成処理]

① 署名対象文書、XML 署名文書に対して実行する変換処理に関する情報、検証時に用いる公開鍵に関する情報を、それぞれ Transforms 要素、KeyInfo 要素に設定する。
② 変換処理に関する情報を元に、署名対象文書の変換処理を行う。
③ ダイジェスト値計算で用いるハッシュ関数のアルゴリズムを、DigestMethod 要素に設定する。さらに、変換した署名対象文書をハッシュ関数で圧縮してダイジェスト値を取得し、DigestValue 要素に設定する。
④ 得られたダイジェスト値を秘密鍵を用いて暗号化して署名値を生成し、SignatureValue 要素に設定する。

以上のプロセスをもとに、XML 署名文書を生成する。

[XML 署名文書の検証処理]

① XML 署名文書の SignatureMethod 要素と KeyInfo 要素から、署名値と公開鍵に関する情報を取得する。
② 公開鍵値で署名値を復号し、ダイジェスト値を取得する。
③ XML 署名文書の Transforms 要素から、変換処理に関する情報を取得して変換処理を実行し、署名対象文書を取得する。
④ 得られた署名対象文書を、XML 署名文書の DigestMethod 要素から取得したハッシュ関数で圧縮し、ダイジェスト値を取得する。
⑤ ②で得られたダイジェスト値と、④で得られたダイジェスト値を比較して、一致すれば検証成功、一致しなければ検証失敗とす

る。

（d）XML 署名機能がサポートしているアルゴリズム

XML 署名文書の生成、検証時に行う処理に関して、XML 署名機能では、表１に示すアルゴリズムをサポートしている。

XML 署名機能では、XML 署名仕様で規定されている、REQUIRED(必須)、RECOMMENDED(推奨)、OPTIONAL(付加的)のすべての標準アルゴリズムをサポートしている。

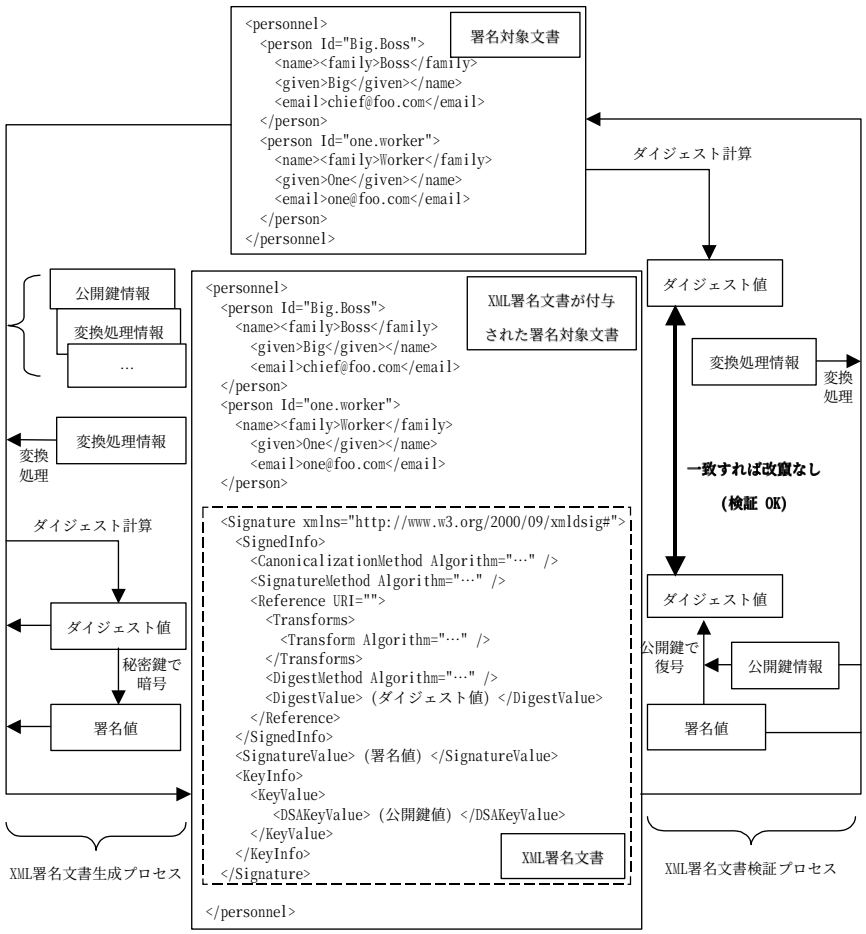

図７．XML 署名文書の生成処理と検証処理のプロセス

アルゴリズムタイプ	関連要素	アルゴリズム	W3C規約要件
ダイジェスト計算	DigestMethod要素	SHA1	REQUIRED
エンコード	Transform要素	Base64	REQUIRED
メッセージ認証コード(共通鍵方式　署名)	SignatureMethod要素	Hmac-SHA1	REQUIRED
公開鍵方式　署名	SignatureMethod要素	DSAwithSHA1(DSS)	REQUIRED
		RSAwithSHA1	RECOMMENDED
正規化	CanonicalizationMethod要素	正規XML(コメント付き)	RECOMMENDED
		正規XML（コメントなし）	REQUIRED
変換	Transform要素	XSLT	OPTIONAL
		Xpath	RECOMMENDED
		Enveloped Signature	REQUIRED

表１．XML 署名機能がサポートしているアルゴリズム

２．２．２　XML 暗号機能

XML 暗号文書は、「暗号対象文書」に XML 暗号機能を施した結果、生成される XML 文書である。XML 暗号文書内部に、暗号化された「暗号対象文書」と「暗号化処理に関する情報」を含む。本技術開発では、「暗号化処理に関する情報」に含まれる「暗号鍵情報」、「暗号化されたコンテンツ」等の情報を XML 文書構造としてどのように格納するかを規定した（２．２．２章（３）（ｄ）参照)。

XML 暗号文書を暗号化、復号処理する処理概要は、それぞれ以下のようになる。

XML 暗号機能の暗号化処理は、まず、「暗号対象部分」を暗号化し「暗号化されたコンテンツ」とする。このとき、「暗号鍵情報」等の暗号化処理の際に指定した情報と一緒に「暗号化処理に関する情報」に格納する。次に、「暗号化処理に関する情報」を「暗号対象文書」中の「暗号対象部分」と置換することによって、XML 暗号文書を生成する。

XML 暗号機能の復号処理は、まず、XML 暗号文書から取り出した「暗号化されたコンテンツ」と「暗号鍵情報」から、元の「暗号対象部分」を復号する。次に、「暗号化処理に関する情報」と置換することにより、暗号対象文書を生成する。

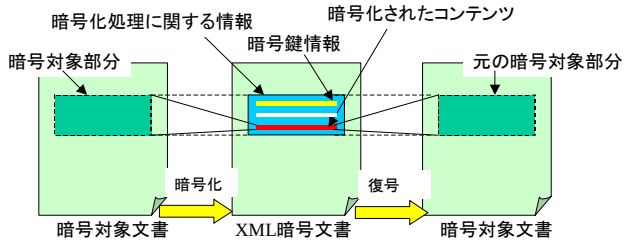

図８．XML 暗号文書の暗号化・復号処理のプロセス

（１）　XML 暗号文書の特徴

本技術開発で開発した XML 暗号文書は、W3C の XML 暗号に関するメーリングリスト上に叩き台として提案された XML 暗号文書の仕様を元にしている。この XML 暗号文書は以下のような特徴を持つ。

- 暗号対象文書が XML 文書である場合、暗号対象部分の柔軟な指定が可能
- 既存の暗号文書形式として高い実績がある CMS(Cryptographic Message Syntax)をベースにした暗号文書形式を提供
- 暗号化処理を必要とする業務アプリケーションの多様な要件を満たすために、柔軟に対応できる文書構造を定義している。具体的には、暗号化された暗号対象文書と暗号化処理に関する情報との包含関係により区別される Embedded, Embedding, Detached の３つの形式の XML 暗号文書形式を提供(２．２．２章（３）（ａ）で詳説)
- 電子文書の本格的運用に伴って、電子文書のアクセス権を制御することが重要となってくる。このような、特定の受取人に対して暗号文書を復号させたいという要件を満たすために、柔軟な暗号鍵情報の添付形式を提供(具体的には EnvelopeInfo 形式と EncryptionInfo 形式を提供。２．２．２章（３）（ｂ）で詳説)

（２）XML 暗号機能の構成

本技術開発で開発を行った XML 暗号機能は暗号対象文書を暗号化して上述の XML 暗号文書を生成し、また生成された XML 暗号文書を復号して、元の暗号対象文書を抽出する機能を提供する。以下の機能から構成される。

①　XML 暗号文書データ管理機能
暗号対象部分を指定して、XML 暗号文書の生成を行う機能である。暗号対象部分の指定や暗号化された電子文書、あるいはそれを復号するのに必要な情報を XML 暗号文書に埋め込む位置を柔軟に指定できる。

②　XML 暗号セキュリティ管理機能
XML 暗号文書の暗号化・復号処理に必要な鍵情報を管理する機能である。

（３）　XML 暗号文書

（ａ）Embedding/Embedded/Detached 形式

XML 暗号文書は暗号化された暗号対象文書とその暗号化処理に関する情報との包含関係により Embedded 形式、Embedding 形式、Detached 形式に分類される。

①　Embedded 形式
暗号化された暗号対象文書の中に、暗号化処理に関する情報が含まれる形式の XML 暗号文書である。
暗号対象文書内に暗号処理に関する情報が埋め込まれる形態となるため、この暗号文書形式の暗号対象文書は XML 文書に限定される。

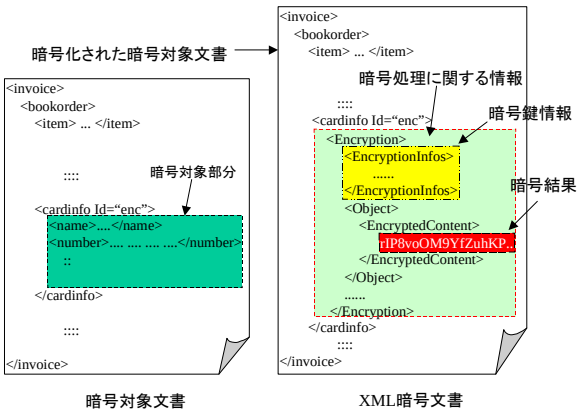

図 9．Embedded 形式の XML 暗号文書

② Embedding 形式

暗号化処理に関する情報の中に暗号化された暗号対象文書が含まれる形式の XML 暗号文書である。

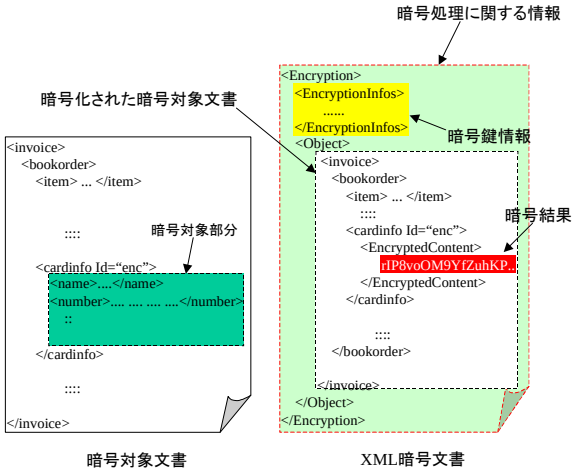

図 10． Embedding 形式の XML 文書

③ Detached 形式

暗号化処理に関する情報と、暗号化された暗号対象文書に包含関係がない XML 暗号文書の形式である。

暗号化処理に関する情報と、暗号化された暗号対象部分を別文書とすることも可能である。

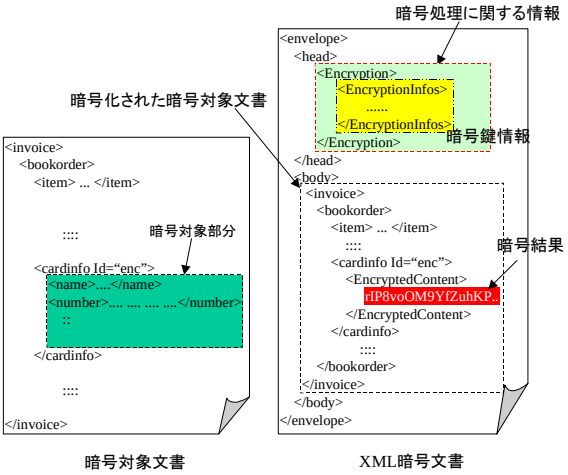

図 11．Detached 形式の XML 暗号文書

（b）EncryptionInfo/EnvelopeInfo 形式

XML 暗号文書は暗号化されたコンテンツを復号するための暗号鍵情報の保持の方法により、EnvelopeInfo 形式と、EncryptionInfo 形式に分類できる。

① EncryptionInfo 形式

暗号対象文書の暗号化に使用した暗号鍵(コンテンツ暗号鍵)を特定する情報のみを格納する形式である。

暗号鍵を送信者、受信者で事前に共有していることを前提とする。単純に XML 暗号文書を二者間で受け渡す場合等に利用する。

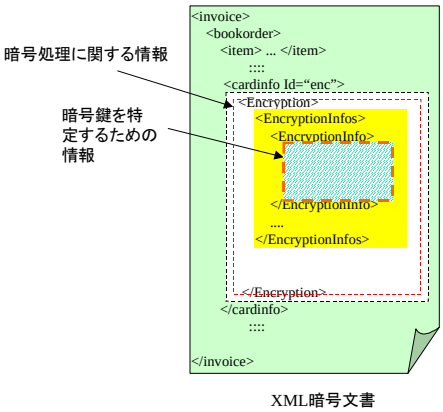

図 12． EncryptionInfo 形式の文書

② EnvelopeInfo 形式

暗号化されたコンテンツを暗号化する際に使用した暗号鍵(コンテンツ暗号鍵)を暗号化し、暗号化処理に関する情報内へ格納する形式である。

使用する鍵配布方式により、さらに、KeyAgree(鍵合意)方式、KeyTrans(鍵転送)方式、KEK(鍵暗号化)方式に細分化できる。

暗号鍵を特定するための情報は、上記の細

分化された各形式に依存し変化する。

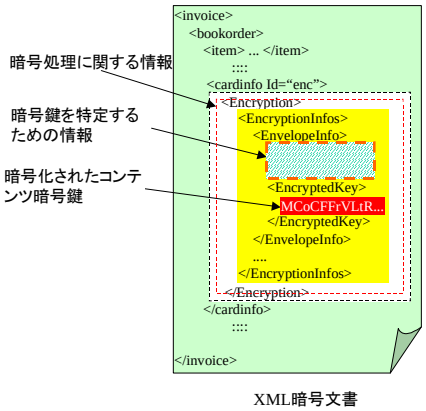

図 １３． EnvelopeInfo 形式の XML 暗号文書

（c）XML 暗号文書がサポートしているアルゴリズム

・ コンテンツ暗号化アルゴリズム
　　Triple-DES CBC PKCS5Padding
・ 鍵配布アルゴリズム(EnvelopeInfo 形式で利用するアルゴリズム)
　　KeyAgree 方式: Deffie-Hellman
　　KeyTrans 方式: RSA
　　KEK 方式: Triple-DES
・ バイナリエンコーディング
　　Base64

（d）XML 暗号文書を構成する XML 要素

Encryption	XML暗号文書のルート要素
EncryptionInfos	暗号化処理に関する情報を保持する要素
EnvelopeInfo	受取人情報と暗号化されたコンテンツを関連付ける要素
RecipientInfos	受取人情報をまとめるための要素
KeyTransRecipientInfo	KeyTrans型の鍵配布方式の受取人情報を保持する要素
RecipientIdentifer	受取人を特定する情報を保持する要素
KeyEncryptionMethod	コンテンツ暗号鍵の暗号化アルゴリズムを保持する要素
EncryptedKey	暗号化された鍵の値を保持する要素
KeyAgreeRecipientInfo	KeyAgree型の鍵配布方式の受取人情報を保持する要素
Originator	差出人公開鍵を特定する情報を保持する要素
UserKeyingMaterial	UserKeyingMaterial情報を保持する要素
KeyEncryptionMethod	コンテンツ暗号鍵の暗号化アルゴリズムを保持する要素
RecipientEncryptedKey	受取人公開鍵と暗号化鍵を関連付ける要素
KeyAgreeRecipientIdentifier	受取人公開鍵を特定する情報を保持する要素
EncryptedKey	暗号化された鍵の値を保持する要素
KEKRecipientInfo	KEK型の鍵配布方式の受取人情報を保持する要素
KEKIdentifier	コンテンツ暗号鍵暗号化鍵を特定する情報
KeyEncryptionMethod	コンテンツ暗号鍵の暗号化アルゴリズムを保持する要素
EncryptedKey	暗号化された鍵の値を保持する要素
EncryptedContentInfo	暗号化処理に関する情報と暗号化されたコンテンツを関連付けるための要素
ContentEncryptionMethod	コンテンツ暗号化アルゴリズムを保持する要素
Reference	暗号化されたコンテンツへの参照を保持する
Object	EncryptedContentを保持する
EncryptedContent	暗号化されたコンテンツを保持する

表 ２．EnvelopeInfo 形式の XML 暗号文書を構成する要素

Encryption	XML暗号のルート要素
EncryptionInfos	暗号化処理に関する情報を保持する要素
Encrypt	対称鍵情報と暗号化されたコンテンツを関連付ける要素
CEKIdentifier	受取人と共有する対称鍵を特定する情報を保持する要素
EncryptedContentInfo	暗号化処理に関する情報と暗号化されたコンテンツを関連付けるための要素
ContentEncryptionMethod	コンテンツ暗号化アルゴリズムを保持する要素
Reference	暗号化されたコンテンツへの参照を保持する
Object	EncryptedContentを保持する
any	暗号化されたコンテンツを保持する

表 ３．EncryptionInfo 形式の XML 暗号文書を構成する要素

３．本年度の活動状況

本技術開発テーマ実施における本年度の活動状況を以下に示す。

（１） XML署名基盤技術開発作業
XML署名機能、および、XML暗号機能からなるXML署名基盤ソフトウェアを開発完了し、２月末に４章で示す成果物一式を提出した。

（２） XML署名ユーザ利用インタフェース仕様検討作業
XML署名基盤ソフトウェアのユーザ利用インタフェースが、W3C XML-Signature Syntax and Processing標準に準拠し、利便性が高く、特定のセキュリティ機能やツールに依存しない汎用性のあるAPIとすることを当初の目的とした。これを達成するため、国内メーカ7社からなるXML署名コンソーシアムを設け、上記観点によりレビューを行ないAPIを策定した。
また、社内の電子政府プロジェクト関連メンバへ、XML署名基盤ソフトのAPI仕様、および、利用イメージ等を提示し、すり合わせを行った。

（３） W3C/IETF評価実験作業
本技術開発を通してW3C/IETF XML Signature Syntax and Processing勧告案の妥当性を確認した。引き続き来年度、XML署名基盤ソフトの相互運用性検証実験を通して、正式勧告策定に貢献していきたい。

（４） リファレンスソフト公開作業
上記作業を通して開発されたXML署名基盤ソフトウェアを情報処理振興事業協会殿の了解を得て標準化団体へリファレンスソフトとして公開する予定である。

４．外部発表および成果物

(1) 外部発表

- 第 19 回 IPA 技術発表会(2000 年 10 月)パネル展示
- 杉山、宮内、森「電子政府プロジェクトにおける XML 署名基盤技術」NEC 技法、Vol.53、No.12
- 杉山、「電子政府における XML 署名基盤技術」情報処理学会中国支部主催 e コマースを担う要素技術と応用講習会
- 杉山、「電子取引文書の改ざんを目的とした XML 電子署名とその応用サービス」NEC 主催 iExpo2000 C&C ユーザフォーラム、J-9

(2) 成果物

本技術開発テーマの成果として本年度納入した物件を以下に示す。

- 外部設計書
- 内部設計書
- ロードモジュール
- ソースコード
- 結合試験仕様書
- 結合試験報告書
- 総合試験仕様書
- 総合試験報告書
- 取扱説明書

５．今後の課題

本技術開発では､相互運用性の確保を目的に XML 署名基盤を開発してきた。しかし、マルチベンダ環境における XML 署名適用という局面において現在､以下のような XML 署名基盤では対処できない非互換性が原因で、異なるシステム間で署名・検証処理が適切に行うことができないという問題がある。

- XML パーサなど､XML 文書を取り扱う際に利用する基盤ソフトウェア間での動作の非互換
- システムが動作するプラットフォーム間での文字コード取り扱い上の非互換

そして、これらは XML 署名を電子申請や電子取引のシステムに適用する際の障害となっており、電子政府システム、電子商取引の普及を促進する上ではこれを必ず解決する必要がある。そのために、異なる基盤ソフトウェア､プラットフォーム間で XML 署名基盤ソフトの互換性検証実験を行い、実験結果に基いて、非互換性を回避するためのガイドラインや事前に非互換部分を発見するテストツールを開発することが重要である。

６． まとめ

本報告書では、XML 署名基盤の技術開発の意義と内容について説明した。また、今年度の活動を通じて達成した成果について報告を行うとともに、今後に残されている課題を明らかにした。来年度以降、これらの課題の解決に取り組み、電子商取引、電子政府の実現に結びつくこれらの基盤の開発に積極的に貢献していく所存である。

７． 参考文献

1) XML-Signature Syntax and Processing, Candidat Recommendation <http://www.w3.org/TR/xmldsig-core/>
2) Canonical XML Version 1.0, W3C Proposed Recommendation <http://www.w3.org/TR/xml-c14n/>
3) RSA Lab PKCS仕様 <http://www.rsasecurity.com/rsalabs/pkcs/>
4) 財団法人 情報処理相互運用技術協会「セキュリティ技術の現状と動向」平成８年３月 （オープンネットワーク化推進のための調査研究報告書 別冊
5) XML Japanese Profile, W3C Note <http://www.w3.org/TR/NOTE-japanese-xml-20000414/>
6) **「電子政府プロジェクトにおける**XML**署名基盤技術」**NEC**技法、**Vol.53**、**No.12
7) Specification of Element-wise XML Encrpytion <http://lists.w3.org/Archives/Public/xml-encryption/2000Aug/att-0005/01-xmlenc-spec.html>
8) XML Encryption Syntax and Processing <http://lists.w3.org/Archives/Public/xml-encryption/2000Aug/att-0001/01-xmlencoverview.html>
9) Cryptographic Message Syntax, RFC2630 <http://www.ietf.org/rfc/rfc2630.txt>